Protecting Critical Assets in Public Clouds

ultima

The growth and popularity of public IaaS continues to drive more data beyond traditional IT security protections – into data centre environments no longer owned, managed or controlled by corporate IT. On-premises IT security controls do not touch the cloud, leaving customer data at risk from the same types of threats targeting assets and applications in corporate data centres. What's more, malware introduced into the cloud can easily propagate among VMs, attack virtual segments or even ride unimpeded over VPN links back to corporate networks.

Public cloud networks are built upon a unified, multi-tenant platform utilising a shared infrastructure to support millions of simultaneous customers worldwide. Foundational to public cloud environments are enhanced security, operational management and threat mitigation practices that protect the infrastructure, cloud fabric, hypervisors, services and tenant environments.

While public cloud providers deliver strong security controls to protect the cloud fabric, they have no knowledge of "normal" customer traffic and thus are unable to determine malicious content from benign. This presents a big challenge to cloud architects and security administrators who are required to provide the same level of security to protect assets in the cloud as if they were on-premises. A defence-in-depth strategy for the cloud should also include protecting all workloads and data from exploits, malware and other sophisticated attacks.

CHECK POINT STARS PARTNER ELITE

The cloud shared responsibility model

To fully embrace the cloud, businesses need to understand where the balance of responsibilities lie between protecting the cloud infrastructure (incumbent upon the cloud provider) and protecting the data that resides in the cloud (incumbent upon the customer). This is what IaaS providers refer to as the shared responsibility model.

Fulfil your shared responsibility with Check Point Cloudguard

To help customers deal with the security issues that fall under their responsibility, Check Point has partnered with the leading public IaaS providers to seamlessly bring the same comprehensive security protections customers enjoy on their premises networks to their cloud environments. Check Point's flagship CloudGuard IaaS Cloud Security solution provides industry-leading threat prevention security to keep customer data in public cloud networks safe from even the most sophisticated attacks. Additionally, Check Point CloudGuard enhances the native segmentation and elastic networking of public IaaS environments to dynamically deliver advanced security and consistent policy enforcement that automatically grows and scales with customer environments while providing reliable and secure connectivity across public and hybrid cloud environments.

Understanding the customer responsibility role versus the role of IaaS providers helps organisations make the best decisions concerning the security of their cloud environments. It also ensures that an organisations cybersecurity strategy efficiently and cost-effectively aligns with the rest of the business goals while delivering consistent protections for all corporate data both on-premises and in the cloud.

Check Point CloudGuard compliments native cloud service provider (CSP) security controls to ensure public IaaS customers can fulfil their shared security responsibilities. With Check Point CloudGuard, customers can secure their workloads and applications running in hybrid and public cloud infrastructures, minimizing threats from breaches, data leakage as well as zero-day threats. Whether your cloud strategy centres around public or hybrid IaaS, VPN replacement, multi-cloud routing, or cloud DMZ, Check Point CloudGuard helps secure all your cloud assets while fully supporting the elastic, dynamic and cost-effective nature of the cloud.

What's more, only Check Point gives you a single pane of glass experience when managing physical, virtual and cloud-based IaaS security, complete with consolidated logs and reporting across all network environments. With Check Point, you can enforce a consistent security policy for corporate assets across both public cloud and on-premises infrastructures, dramatically simplifying compliance with regulatory mandates.

Check Point CloudGuard provides comprehensive threat prevention security, access, identity, strong authentication, compliance reporting and multi-cloud connectivity to help organisations embrace the cloud with confidence. CloudGuard seamlessly integrates with the leading cloud platforms and orchestration tools allowing it to be deployed in minutes while supporting key features such as dynamic security policies and elastic scalability. These powerful capabilities allow you to grow your cloud security elastically with the changing capacity requirements of your dynamic business environment.

Head Office
Gainsborough House
Manor Park, Basingstoke Road
Reading, Berkshire, RG2 0NA

0333 015 8000
enquiries@ultima.com
www.ultima.com

Contact us for more information
0333 015 8000

CHECK POINT CloudGuard

ultima